REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application. The Examiner additionally stated that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are rejected. By this communication, claims 1, 13, 56, and 67 are amended. Hence, claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner noted that any invocations of Official Notice from the previous Office Action that were not explicitly traversed in the amendment of 9/4/08 are now taken as Applicant admissions of prior art, as provided by MPEP 2144.03(c). Applicant responds that all rejections in the previous Office Action were explicitly traversed in the amendment of 9/4/08 and, thus, any of those rejections that to which "Official Notice" was taken.

The Examiner rejected claims 1-6, 11-12, 24-25, 27, 56-60, 66, and 79-83 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al., U.S. Patent 6,789,147 (hereinafter, Kessler) in view of Best, U.S. Patent 4,278,837, (hereinafter, Best). Applicant respectfully traverses the Examiner's rejections.

Regarding claim 1, the Examiner noted that Kessler discloses a (microprocessor) apparatus for performing cryptographic operations comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a microprocessor (col. 4, line 59-col. 5, line 36), said instruction flow comprising an instruction, configured to direct said

microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10); and a cryptography unit, disposed within execution logic in said microprocessor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said microprocessor and coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

The Examiner conceded that the processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred narrow definition of "microprocessor" established in the specification. However, the Examiner asserted that Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 &18). The Examiner also noted that Best clearly discloses wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The Examiner concluded that the claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of

Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Regarding claim 56, the Examiner noted that Kessler discloses an apparatus for performing cryptographic operations, comprising: fetch logic, disposed within a processor, configured to fetch an instruction flow from memory for execution by a processor by said processor (col. 4, line 59 - col. 5, line 36), said instruction flow comprising an instruction, configured to direct said processor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10); translation logic, disposed within said processor, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said one of the cryptographic operation (e.g. col. 8, lines 11-16); and a cryptography unit, disposed within execution logic in said processor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55).

The Examiner stated that the processor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred definition of "microprocessor" established in the specification. However, the Examiner stated that Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, wherein said microprocessor is a hybrid consisting of a conventional microprocessor and a cryptographic coprocessor combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 &18) and, additionally, Best clearly discloses

wherein the microprocessor has a fetch unit disposed within itself configured to fetch an application program from memory by said microprocessor (e.g. col. 6, lines 15-20). The Examiner concluded that the claims are thus obvious because the substitution of Kessler's cryptographic coprocessor in lieu of the default cryptographic coprocessor already disclosed by Best for use as the cryptographic unit of Best's hybrid microprocessor would have yielded predictable results to one of ordinary skill in the art by the time of the instant invention.

Applicant responds that he is convinced that further arguments directed toward distinguishing a microprocessor from a co-processor would be futile, because it is clear that the Examiner is of the opinion that a co-processor is one species of a microprocessor, as would a graphics controller be another species of a microprocessor.

Applicant also respectfully submits that it is his sincere desire to forward this case through the Office in all candor and good faith, and thus he has amended claims 1, 16, and 21 to recite, among other features and limitations, "an x86-compatible microprocessor." This element is clearly defined in the specification, one instance of such is as is stated in paragraph [0041], which is repeated below for ease of reference. To wit (with emphasis provided by underlining):

> **[00410** Referring to FIGURE 3, a block diagram 300 is provided featuring a microprocessor apparatus according to the present invention for performing cryptographic operations. The block diagram 300 depicts a microprocessor 301 that is coupled to a system memory 321 via a memory bus 319. The microprocessor 301 includes translation logic 303 that receives instructions from an instruction register 302. The translation logic 303 comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to translate instructions into associated sequences of micro instructions. The elements employed to perform translation within the translation logic 303 may be shared with other circuits, microcode, etc., that are employed to

perform other functions within the microprocessor 301. According to the scope of the present application, microcode is a term employed to refer to a plurality of micro instructions. A micro instruction (also referred to as a native instruction) is an instruction at the level that a unit executes. For example, micro instructions are directly executed by a reduced instruction set computer (RISC) microprocessor. For a complex instruction set computer (CISC) microprocessor such as an x86-compatible microprocessor, x86 instructions are translated into associated micro instructions, and the associated micro instructions are directly executed by a unit or units within the CISC microprocessor. The translation logic 303 is coupled to a micro instruction queue 304. The micro instruction queue 304 has a plurality of micro instruction entries 305, 306. Micro instructions are provided from the micro instruction queue 304 to register stage logic that includes a register file 307. The register file 307 has a plurality of registers 308-313 whose contents are established prior to performing a prescribed cryptographic operation. Registers 308-312 point to corresponding locations 323-327 in memory 321 that contain data which is required to perform the prescribed cryptographic operation. The register stage is coupled to load logic 314, which interfaces to a data cache 315 for retrieval of data for performance of the prescribed cryptographic operation. The data cache 315 is coupled to the memory 321 via the memory bus 319. Execution logic 328 is coupled to the load logic 314 and executes the operations prescribed by micro instructions as passed down from previous stages. The execution logic 328 comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to perform operations as prescribed by instructions provided thereto. The elements employed to perform the operations within the execution logic 328 may be shared with other circuits, microcode, etc., that are employed to perform other functions within the microprocessor 301. The execution logic 328 includes a cryptography unit 316. The cryptography unit 316 receives data required to perform the prescribed cryptographic operation from the load logic 314. Micro instructions direct the

cryptography unit 316 to perform the prescribed cryptographic operation on a plurality of blocks of input text 326 to generate a corresponding plurality of blocks of output text 327. The cryptography unit 316 comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to perform cryptographic operations. The elements employed to perform the cryptographic operations within the cryptography unit 316 may be shared with other circuits, microcode, etc., that are employed to perform other functions within the microprocessor 301. In one embodiment, the cryptography unit 316 operates in parallel to other execution units (not shown) within the execution logic 328 such as an integer unit, floating point unit, etc. One embodiment of a "unit" within the scope of the present application comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to perform specified functions or specified operations. The elements employed to perform the specified functions or specified operations within a particular unit may be shared with other circuits, microcode, etc., that are employed to perform other functions or operations within the microprocessor 301. For example, in one embodiment, an integer unit comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to execute integer instructions. A floating point unit comprises logic, circuits, devices, or microcode (i.e., micro instructions or native instructions), or a combination of logic, circuits, devices, or microcode, or equivalent elements that are employed to execute floating point instructions. The elements employed execute integer instructions within the integer unit may be shared with other circuits, microcode, etc., that are employed to execute floating point instructions within the floating point unit. In one embodiment that is compatible with the x86 architecture, the cryptography unit 316 operates in parallel with an x86 integer unit, an x86 floating point unit, an x86 MMX® unit,

> and an x86 SSE® unit. According to the scope of the present application, an embodiment is compatible with the x86 architecture if the embodiment can correctly execute a majority of the application programs that are designed to be executed on an x86 microprocessor. An application program is correctly executed if its expected results are obtained. Alternative x86-compatible embodiments contemplate the cryptography unit operating in parallel with a subset of the aforementioned x86 execution units. The cryptography unit 316 is coupled to store logic 317 and provides the corresponding plurality of blocks of output text 327. The store logic 317 is also coupled to the data cache 315, which routes the output text data 327 to system memory 321 for storage. The store logic 317 is coupled to write back logic 318. The write back logic 318 updates registers 308-313 within the register file 307 as the prescribed cryptographic operation is accomplished. In one embodiment, micro instructions flow through each of the aforementioned logic stages 302, 303, 304, 307, 314, 316-318 in synchronization with a clock signal (not shown) so that operations can be concurrently executed in a manner substantially similar to operations performed on an assembly line.

Thus, recitation in the independent claims of "an x86-compatible microprocessor" is submitted to overcome the rejections noted above. By way of summary, in order for any device to be deemed equivalent to an x86-compatible microprocessor as defined above, it must be 1) compatible with the x86 architecture, 2) it must include an x86 integer unit, 3) it must include an x86 floating point unit, 4) it must include an x86 MMX unit, and 5) it must include an x86 SSE unit. In addition, an equivalent device must 6) correctly execute a majority of the application programs that are designed to be executed on an x86 microprocessor.

Applicant has thoroughly studied the teachings of Kessler and Best, both alone and in combination, and finds that Kessler and Best fail to teach any form of an x86-compatible microprocessor. As has been previously submitted, Kessler teaches a security co-processor interface. He does not teach an x86 integer unit, x86 floating point unit, x86 MMX unit, or x86 SSE unit. Kessler fails to teach or suggest the capability to correctly execute a majority of the application programs that are designed to be executed on an x86

microprocessor. Best certainly refers to a "prior art microprocessor," but is entirely vague with regard to what such a microprocessor is. Furthermore, Best is entirely silent with regard to whether such a prior art microprocessor would include an x86 integer unit, x86 floating point unit, x86 MMX unit, or x86 SSE unit. Best fails to teach or suggest the capability to correctly execute a majority of the application programs that are designed to be executed on an x86 microprocessor. To view the teachings of Kessler and best in combination would not yield the limitation that Applicant has added to claims 1 and 56, "an x86-compatible microprocessor," as is defined in the instant specification.

In view of the above points, Applicant respectfully requests that the rejections of claims 1 and 56 be withdrawn.

With respect to claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83, these claims depend from claims 1 and 56 as appropriate, and add further limitations that are neither anticipated nor made obvious by Kessler, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 7-10 and 61-64 under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Best, as noted above, and further in view of "Applied Cryptography, 2nd Edition."

Applicant respectfully traverses the Examiner's rejections and notes that claims 7-10 and 61-64, depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7-10 and 61-64.

The Examiner additionally rejected claims 13-22 and 67-76 under 35 U.S.C. 103(a) as being unpatentable over Kessler and further in view of Johns-Vano et al. (U.S. Patent 6,026,490). Applicant respectfully traverses and notes that claims 13-22 and 67-76 depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record.

Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 13-22 and 67-76.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-22, 24-25, 27, 56-64, 66-76, and 79-83 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

02/25/2009

Date: _____